UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/581,496	06/27/2007	Karthik Kaleedhass	KASS-006-US	3830

62008 7590 11/29/2010

MAIER & MAIER, PLLC
1000 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LEWIS, LISA C	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
11/29/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/581,496	KALEEDHASS ET AL.	
	Examiner	Art Unit	
	Lisa Lewis	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6 and 8-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 8-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Applicant's response with amendments filed 10/25/2010 has been received and entered. Applicant has amended claims 1, 3, 5, 8, 9, 10, 15, 18, 19, 22, 23, and 24, and has cancelled claim 7. Claims 1-6 and 8-24 have been examined the merits.

Response to Arguments

Applicant's arguments have been carefully considered, but are not deemed persuasive, as they still apply. All other arguments have been carefully considered, but are deemed moot in view of the new grounds of rejection presented below.

Applicant argues that Uchida does not teach or suggest encrypting in a dynamic manner the biometric features or that this step is performed prior to a user inputting biometric feature information for authorization.

The examiner respectfully disagrees. The ID and fingerprint come from the encryption unit, and therefore are intended to be encrypted, or at this would have at least been obvious to the skilled artisan for the purpose of basic security -see figure 13, column 2 lines 39-57, column 3 line 64 - column 4 line 18, column 4 line 56 - column 5 line 3, and column 5 lines 17-24, for example. Uchida does not *expressly* teach that the data features are encrypted or that the step is performed before a user inputs their biometric feature for authorization. However, for basic security purposes, and to maintain uniformity throughout the system, the skilled artisan would recognize that it is the intention of Uchida that the features be extracted and encrypted.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-4, 8, 10-20, 23, and 24 are rejected under 35 U.S.C. 103(a), as being unpatentable over Uchida (US 7,246,243) in view of Lindo et al. (US 2002/0099858).

3. Regarding claims 1 and 10, Uchida teaches a method of electronically identifying and verifying an individual utilizing at least one biometric feature of the individual including the steps of:

4. Enrolling an individual into a database including:

a. Inputting required particulars of the individual into the database and ascertaining the existence or otherwise of the particulars of the individual in the database (A user ID and fingerprint are sent to the processor to see if the individual is registered in the system or not) - see figure 13, column 2 lines 39-57, column 3 line 64 - column 4 line 18, column 4 line 56 - column 5 line 3, and column 5 lines 17-24, for example.

b. Capturing biometric features of the individual wherein key features of the biometric raw data are extracted (When a user's fingerprint is captured, features, such as ridge patterns, are extracted) - see figure 13, column 2 lines 39-57, column 3 line 64 - column 4 line 18, column 4 line 56 - column 5 line 3, and column 5 lines 17-24, for example.

c. Encrypting in a dynamic manner the biometric features (The ID and fingerprint come from the encryption unit, and therefore are intended to be encrypted, or at this would have at least been obvious to the skilled artisan for the purpose of basic security) -see figure 13, column 2 lines

39-57, column 3 line 64 - column 4 line 18, column 4 line 56 - column 5 line 3, and column 5 lines 17-24, for example.

d. Transmitting the encrypted data of the biometric features to the server and storing the encrypted data in relation to the particulars of the individual obtained above (The encrypted data is transmitted to an authentication server) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

5. Verifying an individual in the database including:

e. Activating an access apparatus (capable of recording data) with a means to capture at least one biometric feature of an individual in a secure manner using dynamic encryption (A user's fingerprint is detected by a fingerprint sensor and is encrypted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

f. Capturing the biometric feature of an individual wherein key feature of biometric raw data are extracted (A user's fingerprint is captured, and features, such as ridge patterns, of the fingerprint are extracted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

g. Encrypting in a dynamic manner the biometric features (The features are encrypted using a secret key generated by a cipher key generator) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

h. Transmitting the encrypted data of the biometric feature to at least one server (The encrypted data is transmitted to an authentication server) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

i. Verifying the biometric features captured with a pre-stored biometric feature in the server (It is determined whether the received biometrics data has corresponding biometrics data in the database for authentication) - see figure 13, column 5 lines 36-52, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

i. Wherein upon positive identification and verification of the individual access is given to an auxiliary means such as but not limited to access to secured doors, database, computer network, or servers (Access is given to e-commerce over a communications network if the biometric matches a biometric associated with an ID in the database) - see column 1 and column 5 lines 4-16, for example.

6. As discussed above, Uchida teaches that registration is performed into a database by a user supplying their fingerprint and ID to the machine, which is sent to the authentication server for registration, and the data is stored in the server - see column 4 line 56 - column 5 line 3 and column 5 lines 17-24, for example. Uchida does not *expressly* teach that the data features are encrypted or that the step is performed before a user inputs their biometric feature for authorization. However, for basic security purposes, and to maintain uniformity throughout the system, the skilled artisan would recognize that it is the intention of Uchida that the features be extracted and encrypted.

7. Uchida does not teach that the encryption is based on factors including the computing power of the computers and network bandwidth.

8. Lindo et al. teach a method wherein encryption operations may be selected by the user and may be defaulted depending on the available bandwidth - see [0082], for example.

9. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida by allowing the encryption method to be determined based on computing power and available bandwidth, for the purpose of maintaining a functional system without having to perform major system upgrades, based upon the beneficial teachings provided by Lindo et al. These modifications would result in increased power conservation and efficiency, both of which are obvious benefits to the skilled artisan. Additionally, the cited references are in the field of cryptography, as is the current application, and thus, are in analogous arts.

10. Regarding claim 15, Uchida teaches an electronic means of identifying and verifying an individual presenting for such identification and verification including:

j. A means to capture at least one type of biometric features of the individual (A user's fingerprint is detected by a fingerprint sensor and features are extracted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

k. A software means to encrypt in a dynamic manner the biometric features (The features are encrypted using a secret key generated by a cipher key generator) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

l. A transmission means wherein the encrypted biometric features of the individual are transmitted to a server (The encrypted data is transmitted to an authentication server) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

m. A software means to capture the encrypted biometric features presented for identification and verification against stored encrypted biometric features of a purported individual (It is determined whether the received biometrics data has corresponding biometrics data in the database for authentication and identification (A user's identifier ID-A is compared)) - see figure 13, column 5 lines 36-52, column 2 lines 39-57, column 5 lines 4-16, and column 3 line 64 - column 4 line 18, for example.

n. A means to give access to other databases or software if a positive identification and verification is made and to deny such access if a negative identification and verification is made (Access is given to e-commerce over a communications network if the biometric matches a biometric associated with an ID in the database. Denial or authorization is given based on the match) - see column 1, figure 11, and column 5 lines 4-16, for example. Please note that this would inherently require access to some type of software and/or database.

11. Uchida does not teach that the encryption is based on factors including the computing power of the computers and network bandwidth.

12. Lindo et al. teach a method wherein encryption operations may be selected by the user and may be defaulted depending on the available bandwidth - see [0082], for example.

13. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida by allowing the encryption method to be determined based on computing power and available bandwidth, for the purpose of maintaining a functional system without having to perform major system upgrades, based upon the beneficial teachings provided by Lindo et al. These modifications would result in increased power conservation and efficiency, both of which are obvious benefits to the skilled artisan. Additionally, the cited references are in the field of cryptography, as is the current application, and thus, are in analogous arts.

14. Regarding claim 19, Uchida teaches an electronic means of identifying and verifying an individual presenting for such identification and verification including:

o. Access apparatus with a means to capture at least one biometric raw data of an individual in a secure manner using dynamic encryption (A user's fingerprint is detected by a fingerprint sensor and is encrypted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

p. Circuitry to extract any features of the biometric raw data from the means to capture the biometric raw data (A user's fingerprint is captured, and features, such as ridge patterns, of the fingerprint are extracted) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

q. Circuitry to encrypt the key features of the biometric raw data in a dynamic manner (The features are encrypted using a secret key generated by a cipher key generator) - see figure 13 and column 3 line 64 - column 4 line 18, for example.

r. Transmission means to transmit encrypted data of the biometric features to at least one server (The encrypted data is transmitted to an authentication server) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

s. At least one server to receive and store the encrypted data of the biometric feature of the individual (The authentication server stores the received data) - see figure 13, column 2 lines 39-57, and column 3 line 64 - column 4 line 18, for example.

t. Circuitry to verify and/or identify the encrypted data against pre-stored encrypted biometric data in the server (It is determined whether the received biometrics data has corresponding biometrics data in the database for authentication and identification (A user's identifier ID-A is compared)) - see figure 13, column 5 lines 36-52, column 2 lines 39-57, column 5 lines 4-16, and column 3 line 64 - column 4 line 18, for example.

15. Uchida does not teach that the encryption is based on factors including the computing power of the computers and network bandwidth.

16. Lindo et al. teach a method wherein encryption operations may be selected by the user and may be defaulted depending on the available bandwidth - see [0082], for example.

17. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida by allowing the encryption method to be determined based on computing power and available bandwidth, for the purpose of maintaining a functional system without having to perform major system upgrades, based upon the beneficial teachings provided by Lindo et al. These modifications would result in increased power conservation and efficiency, both of which are obvious benefits to the skilled artisan. Additionally, the cited references are in the field of cryptography, as is the current application, and thus, are in analogous arts.

18. Regarding claims 2-4 and 20, Uchida teaches that the server is spatially separated from access apparatus - see figure 13 and column 2 lines 39-56, for example.

19. Regarding claims 11, 16, and 24, Uchida teaches comparing the biometric features with known biometric features from a database and by a PIN (ID) - see - see figure 13, column 5 lines 36-52, column 2 lines 39-57, column 5 lines 4-16, and column 3 line 64 - column 4 line 18, for example.

20. Regarding claims 13, 14, and 23, Uchida teaches that the features are stored at the server itself - see figure 13 and column 2 lines 39-56, for example.

21. Regarding claims 17 and 18, Uchida teaches that the biometric is a fingerprint - see figure 13 and column 3 line 64 - column 4 line 18, for example.

22. Regarding claim 8, Uchida teaches that the particulars are an ID (alpha numeral) - see column 4 line 56 - column 5 line 3 and column 5 lines 17-24, for example.

23. Regarding claim 12, using or eliminating the PIN or user ID is merely a matter of design choice based on security preferences, and is well within the purview of the skilled artisan to discern.

24. Claims 5, 6, and 21 are rejected under 35 U.S.C. 35 U.S.C. 103(a) as being unpatentable over Uchida in view of Lindo et al., and further in view of Bianco et al. (US 6,256,737).

25. The teachings of Uchida and Lindo et al. are relied upon for the reasons set forth above.

26. Regarding claims 5 and 21, Uchida and Lindo et al. do not teach a backup server that the data is rerouted to in a case of failure.

27. Bianco et al. beneficially teach that an alternate biometric server is used as a backup server to biometric data and stores the exact same data so that a server is always available to authenticate users - see column 10 lines 28-35, for example.

28. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida by allowing a backup server to be available in the event of failure, for the purpose of making authentication always available to users, based upon the beneficial teachings provided by Bianco et al. These modifications would result in increased security and efficiency, both of which are obvious benefits to the skilled artisan. Additionally, the cited references are in the field of biometric authentication, as is the current application, and thus, are in analogous arts.

29. Regarding claim 6, Uchida teaches that the server is spatially separated from access apparatus - see figure 13 and column 2 lines 39-56, for example.

30. Claim 9 is rejected under 35 U.S.C. 35 U.S.C. 103(a) as being unpatentable over Uchida in view of Lindo et al., and further in view of McCabe (US 2002/0095317).

31. The teachings of Uchida and Lindo et al. are relied upon for the reasons set forth above.

32. Regarding claim 9, Uchida and Lindo et al. do not teach that the sever is located in a separate country.

33. McCabe beneficially teaches that two backup servers should be used and that one can be located on the opposite end of the country and the other can be located on a different continent - see [0109], for example.

34. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida and Lindo et al. by allowing the server to reside on another country, for the purpose of increased security, based upon the beneficial teachings provided by McCabe. Additionally, the cited references are in the field of computer security, as is the current application, and thus, are in analogous arts.

35. Claim 22 is rejected under 35 U.S.C. 35 U.S.C. 103(a) as being unpatentable over Uchida in view of Lindo et al., and further in view of Robinson et al. (US 2008/0271116).

36. The teachings of Uchida and Lindo et al. are relied upon for the reasons set forth above.

37. Regarding claim 22, Uchida and Lindo et al. do not teach that a token is used in addition to the biometric sample.

38. Robinson et al. beneficially teach that in addition to a biometric sample, a token with identification information can be presented for identification verification - see [0049], for example.

39. It would have been obvious to one of ordinary skill in the art at to create the invention as claimed for the following reasons. It would have been obvious to one of ordinary skill in the art at the time the claimed invention was made to modify the teachings of Uchida and Lindo et al. by allowing a token to be used in addition to the biometrics, for the purpose of increased security and ease of use, based upon the beneficial teachings provided by Robinson et al. Additionally, the cited references are in the field of biometrics, as is the current application, and thus, are in analogous arts.

Conclusion

A reference to specific paragraphs, columns, pages, or figures in a cited prior art reference is not limited to preferred embodiments or any specific examples. It is well settled that a prior art reference, in its entirety, must be considered for all that it expressly teaches and fairly suggests to one having ordinary skill in the art. Stated differently, a prior art disclosure reading on a limitation of Applicant's claim cannot

be ignored on the ground that other embodiments disclosed were instead cited. Therefore, the Examiner's citation to a specific portion of a single prior art reference is not intended to exclusively dictate, but rather, to demonstrate an exemplary disclosure commensurate with the specific limitations being addressed. *In re Heck,* 699 F.2d 1331, 1332-33,216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re *Lemelson,* 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). In re: *Upsher-Smith Labs. v. Pamlab, LLC,* 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005); *In re Fritch,* 972 F.2d 1260, 1264, 23 USPQ2d 1780, 1782 (Fed. Cir. 1992); *Merck & Co. v. Biocraft Labs., Inc.,* 874 F.2d 804,807, 10 USPQ2d 1843, 1846 (Fed. Cir. 1989); *In re Fracalossi,* 681 F.2d 792,794 n.1,215 USPQ 569, 570 n.1 (CCPA 1982); *In re Lamberti, 545 F.2d 747, 750, 192 USPQ 278,280 (CCPA 1976); In re Bozek,* 416 F.2d 1385, 1390, 163 USPQ 545, 549 (CCPA 1969).

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Lisa Lewis whose telephone number is (571) 270-7724. The examiner can normally be reached on Monday - Friday, 6:30 a.m. - 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. L./
Examiner, Art Unit 2436

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436